Theoretical Informatics and Applications
Theoret. Informatics Appl. **35** (2001) 477–490

NOTE ON THE SUCCINCTNESS OF DETERMINISTIC, NONDETERMINISTIC, PROBABILISTIC AND QUANTUM FINITE AUTOMATA *

Carlo Mereghetti[1], Beatrice Palano[2] and Giovanni Pighizzini[3]

Abstract. We investigate the succinctness of several kinds of unary automata by studying their state complexity in accepting the family $\{L_m\}$ of cyclic languages, where $L_m = \{a^{km} \mid k \in \mathbf{N}\}$. In particular, we show that, for any m, *the number of states necessary and sufficient for accepting the unary language L_m with isolated cut point on one-way probabilistic finite automata is $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$, with $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ being the factorization of m*. To prove this result, we give a *general state lower bound for accepting unary languages with isolated cut point on the one-way probabilistic model.* Moreover, we exhibit one-way quantum finite automata that, for any m, accept L_m with isolated cut point and only *two states*. These results are settled within a survey on unary automata aiming to compare the descriptional power of deterministic, nondeterministic, probabilistic and quantum paradigms.

Mathematics Subject Classification. 68Q10, 68Q19, 68Q45.

Keywords and phrases: Deterministic, nondeterministic, probabilistic, quantum unary finite automata.

* *Partially supported by M.I.U.R. COFIN, under the project "Linguaggi formali e automi: teoria e applicazioni". A preliminary version of this paper was presented at the* Third International Workshop on Descriptional Complexity of Automata, Grammars and Related Structures *held in Vienna, Austria, July 20 – 22, 2001.*

[1] Dipartimento di Informatica, Sist. e Com., Università degli Studi di Milano – Bicocca, via Bicocca degli Arcimboldi 8, 20126 Milano, Italy; e-mail: `mereghetti@disco.unimib.it`

[2] Dipartimento di Informatica, Università degli Studi di Torino, c.so Svizzera 185, 10149 Torino, Italy; e-mail: `beatrice@di.unito.it`

[3] Dipartimento di Scienze dell'Informazione, Università degli Studi di Milano, via Comelico 39, 20135 Milano, Italy; e-mail: `pighizzi@dsi.unimi.it`

Introduction

Several characterizations of the class of regular languages in terms of *finite state automata* are studied in the literature. Besides the traditional deterministic and nondeterministic models, alternating, probabilistic and, more recently, quantum finite automata are considered. Equivalence results point out that determinism, nondeterminism and alternation, in one-way or two-way form, exactly capture the class of regular languages [4, 11, 23, 24]. The same happens if we consider one-way probabilistic automata working with isolated cut point [22]. Surprisingly enough (measure-once) one-way quantum finite automata working with isolated cut point are proved to single out a proper subclass of regular languages, namely, group (or reversible) languages [3].

Starting from these considerations, it is natural to investigate the *succinctness* of representing regular languages by using different kinds of automata. In fact, as one may easily argue, their descriptional power turns out to be very different. The first and simplest example of this phenomenon can be observed by comparing one-way deterministic and nondeterministic automata. It is well known that, for any integer n, 2^n states are necessary [16, 18] and sufficient [23] for one-way deterministic automata to simulate n-state one-way nondeterministic automata. A lot of papers tackles this kind of descriptional complexity issues. For instance, the following are the costs, in terms of states, of simulating different n-state automata by one-way deterministic automata [4,22–24]: one-way alternating automata: 2^{2^n}, two-way deterministic automata: n^n, two-way nondeterministic automata: 2^{n^2}, one-way probabilistic automata with ε-isolated cut point: $(1 + 1/(2\varepsilon))^{n-1}$. The optimality of such costs is studied in [1, 4, 16, 18].

Many interesting results are also obtained on the restricted class of *unary automata*, *i.e.*, automata working on a single letter input alphabet. For instance, we know that $\Theta\left(\mathrm{e}^{\sqrt{n \ln n}}\right)$ states are needed to simulate unary n-state one-way nondeterministic or two-way deterministic finite automata by one-way determinism [5]. This simulation cost is extended to two-way nondeterministic finite automata in [15]. Further results concerning acceptance of unary languages are proved in [14] for two-way nondeterministic automata and in [17] for one-way probabilistic automata.

In this paper, we survey and enrich this line of research by exhibiting some other differences in the succinctness of several kinds of automata. In particular, we compare these models by considering their ability of accepting *unary regular languages.*

It is well known that each one-way deterministic and nondeterministic automaton accepting an ultimately properly χ-cyclic unary language[4] must have at least χ states. Here, we show that, *in the case of probabilistic automata working with isolated cut point, this lower bound reduces to* $p_1^{\alpha_1}+p_2^{\alpha_2}+\cdots+p_s^{\alpha_s}$, *where* $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ *is the factorization of* χ. This latter result extends and generalizes to all integers

[4]As we recall in Section 1, a unary language $L \subseteq a^*$ is ultimately properly χ-cyclic if χ is the smallest positive integer such that $a^n \in L \Leftrightarrow a^{n+\chi} \in L$, for any n exceeding a fixed value.

χ and to all unary languages, lower bounds given in [2, 17] for some particular χ-cyclic languages with particular values of χ. It is interesting to observe that the same lower bound holds true for unary *two-way* deterministic and nondeterministic automata [14].

As a further step, we show that our lower bound is *optimal* by using the family $\{L_m\}$ of cyclic languages, with $L_m = \{a^{km} \mid k \in \mathbf{N}\}$. Precisely, for any m, we exhibit a one-way probabilistic automaton that accepts L_m with isolated cut point and exactly $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$ states, being $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$.

Finally, we again use languages L_m to test the effective power of quantum. In fact, we prove that each language L_m can be accepted by a one-way quantum finite automaton with isolated cut point and only *two states*. This result gives added evidence of the fact that, in some cases, quantum machines lead to meaningful advantages when compared with classical computational devices.

The paper is organized as follows: in Section 1, we define the different models of unary automata we shall be dealing with. In Section 2, we first survey known results on the state complexity of one-way and two-way deterministic and nondeterministic unary automata. Then, we prove the above claimed state lower bound for one-way probabilistic automata accepting unary languages with isolated cut point, and its optimality by means of the family $\{L_m\}$. Finally, in Section 3, we exhibit 2-state one-way quantum automata accepting L_m with isolated cut point. An Appendix is added where some operations on one-way quantum automata are introduced. Such operations are needed to show that, by adding one new state, one-way quantum automata can always be regarded as having cut point 1/2 (exactly as in the probabilistic case).

1. Preliminaries

The *greatest common divisor* and *least common multiple* of integers $a_1, \ldots, a_s$ are denoted, respectively, by $\gcd(a_1, \ldots, a_s)$ and $\operatorname{lcm}(a_1, \ldots, a_s)$. We recall that, by the Fundamental Theorem of Arithmetic, any integer $m > 1$ admits a *factorization* as $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, for $p_1, p_2, \ldots, p_s$ primes and $\alpha_1, \alpha_2, \ldots, \alpha_s$ positive integers, which is unique except for the order in which the primes occur. The natural logarithm is denoted by ln.

Given a complex number $z \in \mathbf{C}$, its *complex conjugate* is denoted by z^*, and its *modulus* is $|z| = \sqrt{zz^*}$. Let $\mathcal{V}$ be a vector space of finite dimension n on $\mathbf{C}$. The *inner product* of vectors $x, y \in \mathcal{V}$, with $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, is defined as $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i^*$. The *norm* of x is defined as $\| x \| = \sqrt{\langle x, x \rangle}$.

A complex matrix M is said to be:

Boolean: whenever its entries are either 0 or 1.

Stochastic: whenever its entries are reals from the interval $[0, 1]$ and each row sum equals 1.

Unitary: whenever $MM^H = I = M^H M$, where M^H is the transpose conjugate of M and I is the identity matrix.

In what follows, we quickly outline the types of finite automata we shall be dealing with. For extensive presentations, the reader is referred to [10] for deterministic and nondeterministic automata, to [20] for probabilistic automata, and to [7,8] for quantum automata.

The "hardware" of a *one-way finite automaton* (1fa, for short) $\mathcal{A}$ consists of an input tape which is scanned by an input head moving one position right at each move, plus a finite state control whose states are from the set $\{q_1, q_2, \ldots, q_n\}$. Here, we are interested in $\mathcal{A}$ being a *unary automata*, which means that its input alphabet has a *single letter*, say "a". Unary devices accept *unary languages*, *i.e.*, sets in the form $L \subseteq a^*$. Our unary 1fa $\mathcal{A}$ can be formally written as a triple $\mathcal{A} = (\pi, U, \eta)$, where $\eta \in \{0,1\}^n$ is the characteristic column vector of the final (or accepting) states, while π and U have different forms depending on the nature of $\mathcal{A}$. Precisely, $\mathcal{A}$ can be:

Nondeterministic (1nfa): $\pi \in \{0,1\}^n$ is the characteristic row vector of the initial state, U is an $n \times n$ boolean transition matrix whose (i,j)th entry is 1 if and only if $\mathcal{A}$ moves from the state q_i to the state q_j upon reading "a".

Deterministic (1dfa): as above, except that U is boolean stochastic.

Probabilistic (1pfa): $\pi \in [0,1]^n$ is a stochastic row vector representing the *initial probability distribution* of the states, U is an $n \times n$ stochastic transition matrix whose (i,j)th entry is the *probability* that $\mathcal{A}$ moves from the state q_i to the state q_j upon reading "a".

Quantum (1qfa): $\pi \in \mathbf{C}^n$, with $\| \pi \| = 1$, is the row vector of the *initial amplitudes* of the states, U is an $n \times n$ unitary transition matrix whose (i,j)th entry is a complex number of modulus not exceeding 1 representing the *amplitude* that $\mathcal{A}$ moves from the state q_i to the state q_j upon reading "a".

Let us see how these models accept unary languages. If $\mathcal{A}$ is a unary 1dfa or 1nfa, then *the accepted language* is defined as

$$L_{\mathcal{A}} = \{a^k \mid k \in \mathbf{N} \text{ and } \pi U^k \eta \geq 1\}.$$

For what concerns the probabilistic and quantum paradigms, we first need to define the *acceptance probability* for a string.

Let $\mathcal{A}$ be a unary 1pfa. The probability that $\mathcal{A}$ accepts the input string a^k is defined as

$$p_{\mathcal{A}}(a^k) = \pi U^k \eta.$$

Instead, if $\mathcal{A}$ is a unary 1qfa, such a probability writes as

$$p_{\mathcal{A}}(a^k) = \sum_{\{j \mid \eta_j = 1\}} |(\pi U^k)_j|^2,$$

where the subscript j denotes the jth vector component. For the sake of precision, this way of evaluating the acceptance probability is for *measure-once* 1qfa's [3,19]. In the literature, *measure-many* 1qfa's are also considered [2,3,9] for which the acceptance probability is "slightly more complicated" since it has to be measured

and updated at each step of the computation. In this work, we are concerned only with measure-once model and hence this attribute will always be understood.

Thus, if $\mathcal{A}$ is a 1pfa or 1qfa, *the language accepted by* $\mathcal{A}$ *with cut point* λ is the set

$$L_{\mathcal{A},\lambda} = \{a^k \mid k \in \mathbf{N} \text{ and } p_{\mathcal{A}}(a^k) > \lambda\}.$$

A unary language L is said to be accepted by $\mathcal{A}$ *with isolated cut point* λ, if there exists $\varepsilon > 0$ such that, for any $a^k \in L$ ($a^k \notin L$), we have $p_{\mathcal{A}}(a^k) \geq \lambda + \varepsilon$ ($\leq \lambda - \varepsilon$). In the literature of 1pfa's, it is customarily assumed $\lambda = 1/2$ which is not a severe assumption since any 1pfa can always be transformed into an equivalent 1pfa having cut point $1/2$ (maintaining isolation around the cut point, if it exists) by adding one new state. This fact can be proved by using standard composition operations on 1pfa's [20]. In the Appendix, we show how to adapt such composition operations to the quantum case. This enables us to prove that even 1qfa's can always be transformed into equivalent 1qfa's having cut point $1/2$ provided we add one new state.

It is well known that the class of languages accepted with isolated cut point on 1pfa's coincides with that of regular languages [22]. On the other hand, quite surprisingly, we know from [3] that the class of languages accepted with isolated cut point on 1qfa's is a *proper subclass* of regular languages, namely, group (or reversible) languages [21].

We will also consider *two-way deterministic and nondeterministic automata* (2dfa's and 2nfa's, resp.). Without going into the details of their definition, for which the reader is referred to [10], we just recall that two-way automata are the natural generalization where the input head is allowed to move back and forth on the input tape.

A unary language L is χ-*cyclic*, for some integer $\chi > 0$, whenever, for any $n \geq 0$, $a^n \in L$ if and only if $a^{n+\chi} \in L$. Moreover, L is *properly* χ-*cyclic* if and only if it is χ-cyclic, but not χ'-cyclic, for any $\chi' < \chi$.

It is well-known that (infinite) unary regular languages form *ultimately periodic sets*, as stated in the following

Theorem 1.1. *Let L be a unary regular language. Then, there exist two integers $\nu \geq 0$, $\chi > 0$ such that, for any $n \geq \nu$, $a^n \in L$ if and only if $a^{n+\chi} \in L$.*

To emphasize the periodicity of a language L as in Theorem 1.1, we say that L is *ultimately* χ-*cyclic*. L is *properly ultimately* χ-*cyclic* if and only if it is ultimately χ-cyclic, but not ultimately χ'-cyclic, for any $\chi' < \chi$. Notice that L is accepted by a 1dfa whose transition digraph consists of a path of ν states joined to a cycle of χ states.

As a consequence of simulation results in [5, 15], if L is accepted by a 1nfa or 2nfa with n states, then we can assume $\nu = O(n^2)$ and $\chi = O\left(\mathrm{e}^{\sqrt{n \ln n}}\right)$. On the other hand, in [17] it is proved that, for some languages accepted with isolated cut point by n-state 1pfa's, χ has the same upper limitation but ν can be dramatically bounded, namely, by a constant.

2. Comparing the size of deterministic, nondeterministic and probabilistic automata. An optimal lower bound for 1pfa's

In this section, we start analyzing how the number of states may vary by using deterministic, nondeterministic and probabilistic automata to accept unary inputs. As benchmark languages, we consider a very simple family of cyclic languages.

For any $m > 1$, we let

$$L_m = \{a^{km} \mid k \in \mathbf{N}\}.$$

As a general result, one can easily state the following optimal bound on the size of the simplest machines we are considering:

Proposition 2.1. *For any integer $m > 0$, m states are necessary and sufficient for accepting L_m on 1dfa's and 1nfa's.*

For more sophisticated automata, the number of states necessary and sufficient for L_m is known for *particular* values of m.

For *prime* m, the results are summarized in the following:

Theorem 2.2. *For any prime p, p states are necessary and sufficient for accepting L_p on*

- *2dfa's and 2nfa's* [14]*;*
- *1pfa's with isolated cut point* [2]*.*

In other words, Theorem 2.2 says that L_p is "so hard" that neither two-way motion nor nondeterminism nor probabilism can help in lowering the number of states of the trivial 1dfa for L_p consisting of a simple cycle of p states.

On the other hand, there exists a family of L_m languages for which two-way motion or probabilism exponentially decreases the number of states. To define such a family, we need the function

$$F(n) = \max\{\mathrm{lcm}(x_1, \dots, x_s) \mid x_1, \dots, x_s > 0 \text{ are integers and } x_1 + \cdots + x_s = n\}.$$

This function is well known in the realm of combinatorics [12, 13, 26], and has a great importance in the study of simulation costs between unary automata [5, 15]. Evaluating its growth rate is known as Landau's problem [12, 13, 25, 26]. Several approximations for $F(n)$ are given in the literature. The best one is contained in [25] and leads to the following estimation which suffices to our purposes:

Lemma 2.3. $F(n) = \Theta\left(\mathrm{e}^{\sqrt{n \ln n}}\right)$.

We also recall from [25] that $F(n)$ attains its maximal values on $x_1, \dots, x_s$ being mutually coprime.

Now, we are ready to introduce the family $\{L_{F(n)}\}$ for which the following state requirements are known from the literature:

Theorem 2.4. *For any integer $n > 0$, n states are necessary and sufficient for accepting $L_{F(n)}$ on*

- *2dfa's and 2nfa's* [14]*;*
- *1pfa's with isolated cut point* [17]*.*

Summing up, we have singled out two paradigmatic opposite situations. In the first one, corresponding to languages L_p, automata added features do not yield smaller devices at all. In the second, corresponding to languages $L_{F(n)}$, two-way motion and probabilism lead to automata which are exponentially more succinct.

At this point, a natural question arises: what can we say on the size of automata accepting languages L_m *when no particular form is assumed for* m? The answer is provided in [14] for two-way deterministic and nondeterministic automata (in what follows, $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ denotes integer factorization):

Theorem 2.5. *For any integer $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, the number of states necessary and sufficient for accepting L_m on 2dfa's and 2nfa's is $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$.*

Thus, we are left to examine the size of 1pfa's accepting L_m with isolated cut point. To this purpose, we are now going to prove a *state lower bound for 1pfa's accepting general unary languages with isolated cut point.* Then, we will design a minimal 1pfa that accepts L_m with isolated cut point, and whose size matches such a lower bound thus witnessing its optimality.

As it can be shown, the results in the literature collected in Theorem 2.2 and in Theorem 2.4 concerning the optimal size of 1pfa's accepting L_m, for particular values of m, turn out to be a direct consequence of what we are about to prove.

We begin with some considerations on the structure of 1pfa's (see [20]). A unary 1pfa $\mathcal{A} = (\pi, U, \eta)$ is basically a (homogeneous) Markov chain. Hence, we can classify its states as *transient* or *ergodic*: a state q is *transient* if and only if there exists a state $p \neq q$ such that p is reachable from q (by reading some input symbols), but q is not reachable from p. If q is not transient, then it is *ergodic.* The set of ergodic states is partitioned into *ergodic classes*: two ergodic states q and p belong to the same class if and only if p can be reached from q.

We can associate with the 1pfa $\mathcal{A} = (\pi, U, \eta)$ the transition graph $G = (Q, E)$, where $Q = \{q_1, q_2, \ldots, q_n\}$ is the set of states of $\mathcal{A}$, and $E \subseteq Q \times Q$ is the set of pairs (q_i, q_j) such that the (i, j)th entry of U is greater than 0, *i.e.*, there is a nonzero probability of reaching q_j from q_i upon reading an input symbol. Hence, the ergodic classes are easily seen to be the *strongly connected components* of the graph obtained from G by restricting to ergodic states. The *period* of an ergodic class is the greatest common divisor of the lengths of the cycles in the

corresponding strongly connected component. It suites our goal to prove that:

Lemma 2.6. *Given an n-state 1pfa $\mathcal{A} = (\pi, U, \eta)$, let $\{d_1, d_2, \ldots, d_k\}$ be the set of periods of its ergodic classes. Then:*

(i) $d_1 + d_2 + \cdots + d_k \leq n$;

(ii) if $\mathcal{A}$ accepts a language L with cut point λ isolated by ε, then L is ultimately d-cyclic, for $d = \mathrm{lcm}(d_1, d_2, \ldots, d_k)$.

Proof. Point (i) follows trivially from the graph-theoretic view of ergodic classes given before this lemma.

For point (ii), we use an approach similar to that adopted in the proof of [17] (Th. 5). We mainly need a property of stochastic matrices (see, *e.g.* [6]) which, applied to our 1pfa $\mathcal{A}$, ensures the existence of the limit matrix

$$\mathcal{U} = \lim_{m \to \infty} (U^d)^m. \tag{1}$$

Such a limit implies the following fact: for each $1 \leq i, j \leq n$, let ${U^{dm}}_{ij}$ ($\mathcal{U}_{ij}$) denote the (i,j)th entry of U^{dm} ($\mathcal{U}$). Then, for any $\delta > 0$, there exists an integer $\overline{m}$ such that, for any $m > \overline{m}$, we have $|{U^{dm}}_{ij} - \mathcal{U}_{ij}| < \delta$. Roughly speaking, for sufficiently large values of m, we can substitute U^{dm} with $\mathcal{U}$ "committing an arbitrarily small error."

Let a^m be an input string for the 1pfa $\mathcal{A}$. By definition, $\mathcal{A}$ accepts a^m with probability $p_{\mathcal{A}}(a^m) = \pi U^m \eta$. We can obviously write m as $m = d\lfloor m/d \rfloor + r$, with $r = m \bmod d$, and this yields

$$\pi U^m \eta = \pi U^{d\lfloor m/d \rfloor + r} \eta = \pi U^{d\lfloor m/d \rfloor} U^r \eta.$$

By considering this equation in the light of limit (1), we get the existence of an integer $\tilde{m}$ such that, for any $m > \tilde{m}$

$$|\pi U^m \eta - \pi \mathcal{U} U^r \eta| = |\pi U^{d\lfloor m/d \rfloor} U^r \eta - \pi \mathcal{U} U^r \eta| < \varepsilon, \tag{2}$$

where ε is the radius of the interval which isolates cut point λ on our 1pfa $\mathcal{A}$.

Let us repeat this reasoning by giving the string a^{m+d} as input to $\mathcal{A}$. The probability that $\mathcal{A}$ accepts a^{m+d} now writes as $p_{\mathcal{A}}(a^{m+d}) = \pi U^{m+d} \eta$. By observing that $(m+d) \bmod d = m \bmod d = r$, we can write $m + d = d\lfloor (m+d)/d \rfloor + r$, and this yields

$$\pi U^{m+d} \eta = \pi U^{d\lfloor (m+d)/d \rfloor + r} \eta = \pi U^{d\lfloor (m+d)/d \rfloor} U^r \eta.$$

Again, this equation can be seen in the light of limit (1) thus obtaining that, for any $m > \tilde{m}$

$$|\pi U^{m+d} \eta - \pi \mathcal{U} U^r \eta| = |\pi U^{d\lfloor (m+d)/d \rfloor} U^r \eta - \pi \mathcal{U} U^r \eta| < \varepsilon. \tag{3}$$

By considering inequalities (2) and (3) at once, one easily gets that, for any $m > \tilde{m}$

$$|\pi U^m \eta - \pi U^{m+d} \eta| < 2\varepsilon. \tag{4}$$

Now, recall that $\mathcal{A}$ accepts the language L with cut point λ isolated by ε. This, by definition, means that, for any m

$$|p_{\mathcal{A}}(a^m) - \lambda| = |\pi U^m \eta - \lambda| > \varepsilon,$$

which, together with (4), easily leads to obtain that, for any $m > \tilde{m}$

$$\underbrace{\pi U^m \eta}_{p_{\mathcal{A}}(a^m)} > \lambda \quad \text{if and only if} \quad \underbrace{\pi U^{m+d} \eta}_{p_{\mathcal{A}}(a^{m+d})} > \lambda.$$

In other words, we have proved that, for any $m > \tilde{m}$, the string a^m belongs to L if and only if a^{m+d} belongs to L. So L is ultimately d-cyclic. □

At this point, we are ready to prove the claimed general state lower bound for 1pfa's accepting unary languages with isolated cut point:

Theorem 2.7. *Let L be a unary language which is ultimately properly χ-cyclic, with $\chi = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Then, the number of ergodic states of any 1pfa accepting L with isolated cut point is at least $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$.*

Proof. Suppose that L is accepted with isolated cut point by a 1pfa $\mathcal{A}$ having n ergodic states. From Lemma 2.6, we get that L *is ultimately d-cyclic*, where $d = \operatorname{lcm}(d_1, d_2, \ldots, d_k)$, d_i is the period of the ith ergodic class of $\mathcal{A}$, and $d_1 + d_2 + \cdots + d_k \leq n$. On the other hand, L is ultimately *properly* χ-cyclic. Hence, χ must divide d, *i.e.*

$$\operatorname{lcm}(d_1, d_2, \ldots, d_k) = d = h\chi = h\, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

for some $h \geq 1$. By this equation and the definition of lcm, we can write

$$\operatorname{lcm}(d_1, d_2, \ldots, d_k) = \prod_{i=1}^{t} p_i^{\gamma_i} = h\, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

for a suitable $t \geq s$ and $\gamma_i = \max\{\log_{p_i} d_j \mid 1 \leq j \leq k \text{ and } p_i \text{ divides } d_j\}$ denoting the highest power of prime p_i in the factorizations of $d_1, d_2, \ldots, d_k$. Thus, for each $1 \leq i \leq s$, $p_i^{\alpha_i}$ divides the corresponding $p_i^{\gamma_i}$ which, in turn, is a factor of some of d_j's, and this clearly implies that $p_i^{\alpha_i} \leq d_j$ for some $1 \leq j \leq k$. It may happen that two or more $p_i^{\alpha_i}$'s divide the same d_j. In this case, such $p_i^{\alpha_i}$'s being mutually coprime divisors of d_j, their sum does not exceed d_j itself.

All this reasoning enables us to bound above the sum of $p_i^{\alpha_i}$'s as

$$n \geq d_1 + d_2 + \cdots + d_k \geq p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s},$$

whence the claimed result follows. □

Let us now turn to 1pfa's accepting languages L_m with isolated cut point. Clearly, we can apply Theorem 2.7 and obtain the following state lower bound:

> *For any integer $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, any 1pfa accepting L_m with isolated cut point must have at least $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$ ergodic states.*

Yet, $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$ *states are also sufficient.* We are going to show this by informally designing a 1pfa $\mathcal{A}$ accepting L_m with isolated cut point and exactly $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$ states.

The transitions of $\mathcal{A}$ are deterministic. In particular, its states are arranged into s disjoint cycles $C_1, C_2, \ldots, C_s$ of lengths $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$, respectively. On each cycle C_j, a state c_j is chosen as initial and final state, while all the other states are nonfinal. Hence, the cycle C_j can be seen as a $p_j^{\alpha_j}$-state 1dfa accepting strings whose lengths are multiple of $p_j^{\alpha_j}$. Finally, $\mathcal{A}$ has an initial distribution which assigns probability $1/s$ with the initial state of each cycle, namely states $c_1, c_2, \ldots, c_s$, and null probabilities to the remaining states.

Consider the input string a^n. If n is a multiple of m, *i.e.*, a multiple of each $p_j^{\alpha_j}$, then a^n is easily seen to be accepted by $\mathcal{A}$ with probability 1. On the other hand, if m does not divide n, then there must exist at least one cycle C_j which does not accept a^n. Hence, it is not hard to see that the probability that $\mathcal{A}$ accepts a^n cannot exceed $1 - 1/s$. Thus, by setting $\lambda = 1 - \frac{1}{2s}$, we can conclude that $\mathcal{A}$ accepts L_m with cut point λ isolated by $\varepsilon = \frac{1}{2s}$ and $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$ states, all of which are easily seen to be ergodic. It may be worth noting that ε is inversely proportional to the number of factors of m.

All this reasoning proves the following theorem which also shows that *the optimality of the lower bound given in Theorem 2.7 is witnessed by languages L_m*:

Theorem 2.8. *For any integer $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, the number of states necessary and sufficient for accepting L_m with isolated cut point on 1pfa's is $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$.*

3. Two states are enough for accepting L_m on quantum automata

To sum up the results so far obtained, we have that:

> *For any integer $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, accepting L_m requires exactly m states on 1dfa's and 1nfa's, while $p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_s^{\alpha_s}$ states are necessary and sufficient on 2dfa's, 2nfa's, and 1pfa's with isolated cut point.*

In this section, we show that adopting the quantum paradigm on 1fa's leads to incredibly small devices for L_m. In fact:

Theorem 3.1. *For any integer $m > 0$, L_m can be accepted with isolated cut point by a 1qfa with two states.*

Proof. We use a construction which is similar to that presented in [2]. We define the 2-state 1qfa

$$\mathcal{A} = \left(\pi = (1,0), U = \begin{pmatrix} \cos\frac{\pi}{m} & i\sin\frac{\pi}{m} \\ i\sin\frac{\pi}{m} & \cos\frac{\pi}{m} \end{pmatrix}, \eta = (1,0) \right).$$

One can easily verify that U is a unitary matrix, and that

$$U^n = \begin{pmatrix} \cos\frac{\pi n}{m} & i\sin\frac{\pi n}{m} \\ i\sin\frac{\pi n}{m} & \cos\frac{\pi n}{m} \end{pmatrix}.$$

Thus, as stated in Section 1, the probability that $\mathcal{A}$ accepts the string a^n amounts to

$$p_{\mathcal{A}}(a^n) = \sum_{\{j \mid \eta_j = 1\}} |(\pi U^n)_j|^2 = \cos^2\left(\frac{\pi n}{m}\right).$$

Such $p_{\mathcal{A}}$ is a function of period m, *i.e.*, $p_{\mathcal{A}}(a^n) = p_{\mathcal{A}}(a^{n+m})$ for any $n \geq 0$, and its maximum value 1 is attained if and only if n is a multiple of m. Moreover, it is not hard to see that, on n's which are not multiple of m, we have $p_{\mathcal{A}}(a^n) \leq p_{\mathcal{A}}(a) < 1$. In other words, our 1qfa $\mathcal{A}$ accepts with certainty the strings in L_m, while the acceptance probability for the strings not in L_m is bounded above by $p_{\mathcal{A}}(a) < 1$.

Thus, we can set $\lambda = (1+p_{\mathcal{A}}(a))/2$ and $\varepsilon = (1-p_{\mathcal{A}}(a))/2$, and conclude that L_m is accepted by the 2-state 1qfa $\mathcal{A}$ with cut point λ isolated by ε. It may be worth noting that ε is asymptotically inversely proportional to m, for $m \to +\infty$. □

We would like to end with a quick comment emphasizing how the nature of automata evolution influences the size of automata.

The 1qfa $\mathcal{A}$ that we construct in the proof of Theorem 3.1 is "parametrized by m", in the sense that m shows up explicitly in the amplitudes of the transition matrix U. So, the quantum paradigm enables us to transfer information on the language, namely m, directly into automaton evolution. Moreover, we are also able to fully take advantage of this fact since the resulting automaton is incredibly small.

Something similar, but less evident, happens with probabilistic mode. Even in the 1pfa for L_m built in Section 2 we store some information on L_m into automaton dynamics. In fact, what explicitly appears is the number s of prime factors of m that fixes the initial probability distribution. Again, the resulting automaton is smaller than 1dfa's or 1nfa's for L_m.

On the contrary, deterministic and nondeterministic paradigms have such a "simple" dynamics that the only place to store information on L_m is the set of states, preparing exactly m states.

Appendix

Here, we prove that any 1qfa working with a given isolated cut point can always be transformed into an equivalent 1qfa with isolated cut point $1/2$ by adding only one new state. We prove this property for unary 1qfa's, but its extension to 1qfa's working on general input alphabets is straightforward.

We first need some operations on 1qfa's. Recall that with $p_{\mathcal{A}} : \mathbf{N} \to [0,1]$ we denote the acceptance probability of the 1qfa $\mathcal{A} = (\pi, U, \eta)$ defined, for any $n \in \mathbf{N}$, as $p_{\mathcal{A}}(a^n) = \sum_{\{j \mid \eta_j = 1\}} |(\pi U^n)_j|^2$.

Proposition 3.2. *Let $\mathcal{A} = (\pi_{\mathcal{A}}, U_{\mathcal{A}}, \eta_{\mathcal{A}})$ and $\mathcal{B} = (\pi_{\mathcal{B}}, U_{\mathcal{B}}, \eta_{\mathcal{B}})$ be two 1qfa's.*

(i) There exists a 1qfa $\overline{\mathcal{A}}$ with the same number of states as $\mathcal{A}$ such that $p_{\overline{\mathcal{A}}} = 1 - p_{\mathcal{A}}$.

(ii) For any nonnegative reals α, β satisfying $\alpha + \beta = 1$, there exists a 1qfa $\alpha\mathcal{A} + \beta\mathcal{B}$ such that $p_{\alpha\mathcal{A}+\beta\mathcal{B}} = \alpha p_{\mathcal{A}} + \beta p_{\mathcal{B}}$, and whose number of states is the sum of the number of states of $\mathcal{A}$ plus the number of states of $\mathcal{B}$.

Proof.

(i) Define $\overline{\mathcal{A}} = (\pi_{\mathcal{A}}, U_{\mathcal{A}}, \neg\eta_{\mathcal{A}})$, where $\neg\eta$ is the bitwise negation of η.

(ii) Define $\alpha\mathcal{A} + \beta\mathcal{B} = ((\sqrt{\alpha}\pi_{\mathcal{A}}, \sqrt{\beta}\pi_{\mathcal{B}}), U_{\mathcal{A}} \oplus U_{\mathcal{B}}, (\eta_{\mathcal{A}}, \eta_{\mathcal{B}}))$, where

$$U_{\mathcal{A}} \oplus U_{\mathcal{B}} = \begin{pmatrix} U_{\mathcal{A}} & \mathbf{0} \\ \mathbf{0} & U_{\mathcal{B}} \end{pmatrix}$$

is the direct sum of the matrices $U_{\mathcal{A}}$ and $U_{\mathcal{B}}$.

In both cases, it is easy to verify that we construct a well-defined 1qfa inducing the desired acceptance probability. □

These operations enable us to show that:

Proposition 3.3. *For any unary language L accepted by a 1qfa $\mathcal{A}$ with cut point λ isolated by ε, there exists a 1qfa $\mathcal{C}$ accepting L with isolated cut point $1/2$ and one new state more than $\mathcal{A}$.*

Proof. In what follows, we use the 1-state 1qfa $\mathcal{U} = ((1), \mathbf{1}, (1))$ whose acceptance probability is $p_{\mathcal{U}}(a^n) = 1$, for each $n \in \mathbf{N}$. Two cases arise in our proof, depending on the value of λ:

- $\lambda < 1/2$: By Proposition 3.2(ii), we can construct the 1qfa

$$\mathcal{C} = \frac{1}{2(1-\lambda)}\mathcal{A} + \frac{1-2\lambda}{2(1-\lambda)}\mathcal{U}.$$

  It is easy to see that $\mathcal{C}$ accepts L with cut point $1/2$ isolated by $\varepsilon/(2(1-\lambda))$.
- $\lambda > 1/2$: By Proposition 3.2(i), we can construct the 1qfa $\overline{\mathcal{A}}$ accepting the complement language $L^c = \{a\}^* \setminus L$ with cut point $\overline{\lambda} = 1 - \lambda < 1/2$ isolated by ε. Now, we can operate as in the previous point, thus using

Proposition 3.2(ii) to construct the 1qfa

$$\overline{\mathcal{C}} = \frac{1}{2(1-\overline{\lambda})}\overline{\mathcal{A}} + \frac{1-2\overline{\lambda}}{2(1-\overline{\lambda})}\mathcal{U}.$$

Such a 1qfa accepts the language L^c with cut point $1/2$ isolated by $\varepsilon/(2(1-\overline{\lambda}))$. In turn, it is easy to verify that $\mathcal{C} = \overline{\overline{\mathcal{C}}}$ is easily seen to accept L with cut point $1/2$ isolated by $\varepsilon/(2(1-\overline{\lambda}))$.

In both cases, the resulting 1qfa $\mathcal{C}$ has only one new state more than $\mathcal{A}$, as one may easily verify by considering Proposition 3.2. □

References

[1] A. Ambainis, The complexity of probabilistic *versus* deterministic finite automata, in *Proc. 7th International Symposium on Algorithms and Computation* (ISAAC). Springer, *Lecture Notes in Comput. Sci.* **1178** (1996) 233-238.

[2] A. Ambainis and R. Freivalds, 1-way quantum finite automata: Strengths, weaknesses and generalizations, in *Proc. 39th Annual Symposium on Foundations of Computer Science* (FOCS). IEEE Computer Society Press (1998) 332-342.

[3] A. Brodsky and N. Pippenger, *Characterizations of 1-way quantum finite automata,* Techn. Rep. 99-03. Univ. of British Columbia, Dept. of Computer Science (1999).

[4] A. Chandra, D. Kozen and L. Stockmeyer, Alternation. *J. ACM* **28** (1981) 114-133.

[5] M. Chrobak, Finite automata and unary languages. *Theoret. Comput. Sci.* **47** (1986) 149-158.

[6] F. Gantmacher, *Applications of Theory of Matrices*. Interscience Pub., New York (1959).

[7] J. Gruska, *Quantum Computing*. McGraw-Hill, London, New York (1999).

[8] J. Gruska, Descriptional complexity issues in quantum computing. *J. Autom. Lang. Comb* **5** (2000) 191-218.

[9] A. Kondacs and J. Watrous, On the power of quantum finite state automata, in *Proc. 38th Annual Symposium on Foundations of Computer Science* (FOCS). IEEE Computer Society Press (1997) 66-75.

[10] J. Hopcroft and J. Ullman, *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, Reading, MA (1979).

[11] R. Ladner, R. Lipton and L. Stockmeyer, Alternating pushdown and stack automata. *SIAM J. Comput.* **13** (1984) 135-155.

[12] E. Landau, Uber die Maximalordung der Permutationen gegebenen Grades. *Archiv. der Math. und Phys.* **3** (1903) 92-103.

[13] E. Landau, *Handbuch der lehre von der verteilung der primzahlen.* I. Teubner, Leipzig, Berlin (1909).

[14] C. Mereghetti and G. Pighizzini, Two-Way automata simulations and unary languages. *J. Autom. Lang. Comb.* **5** (2000) 287-300.

[15] C. Mereghetti and G. Pighizzini, Optimal simulations between unary autom. *SIAM J. Comput.* **30** (2001) 1976-1992.

[16] A. Meyer and M. Fischer, Economy of description by automata, grammars, and formal systems, in *Proc. 12th Annual Symposium on Switching and Automata Theory*. East Lansing, Michigan (1971) 188-191.

[17] M. Milani and G. Pighizzini, Tight bounds on the simulation of unary probabilistic automata by deterministic automata, in *Pre-Proc. Descriptional Complexity of Automata, Grammars and Related Structures* (DCAGRS), Techn. Rep. 555. Univ. of Western Ontario, Canada, Dept. Comp. Sci., *J. Autom. Lang. and Comb.* (2000).

[18] E. Moore, On the bounds for state-set size in the proofs of equivalence between deterministic, nondeterministic, and two-way finite automata. *IEEE Trans. Comput.* **C-20** (1971) 1211-1214.
[19] C. Moore and J. Crutchfield, Quantum automata and quantum grammars. *Theoret. Comput. Sci.* **237** (2000) 275-306.
[20] A. Paz, *Introduction to Probabilistic Automata*. Academic Press, New York, London (1971).
[21] J.E. Pin, On Languages Accepted by finite reversible automata, in *Proc. of the 14th International Colloquium on Automata, Languages and Programming* (ICALP). Springer-Verlag, *Lecture Notes in Comput. Sci.* **267** (1987) 237-249.
[22] M. Rabin, Probabilistic automata. *Inform. and Control* **6** (1963) 230-245.
[23] M. Rabin and D. Scott, Finite automata and their decision problems. *IBM J. Res. Develop.* **3** (1959) 114-125. Also in: E.F. Moore, *Sequential Machines: Selected Papers*. Addison-Wesley, Reading, MA (1964).
[24] J. Shepherdson, The reduction of two-way automata to one-way automata. *IBM J. Res. Develop.* **3** (1959) 198-200. Also in: E.F. Moore, *Sequential Machines: Selected Papers*. Addison-Wesley, Reading, MA (1964).
[25] M. Szalay, On the maximal order in S_n and S_n^*. *Acta Arithmetica* **37** (1980) 321-331.
[26] P. Turán, Combinatorics, partitions, group theory, edited by B. Serge, *Colloquio Internazionale sulle Teorie Combinatorie*. Acc. Naz. dei Lincei, Rome (1976) 181-200.

Communicated by J. Hromkovic.
Received December 13, 2001. Accepted March 15, 2002.